

UNITED STATES DISTRICT COURT

for the
Eastern District of Michigan

In the Matter of the Search of)
 (Briefly describe the property to be searched)
 or identify the person by name and address))
 INFORMATION ASSOCIATED WITH APPLE ID)
 tsyxxx@aol.com THAT IS STORED AT PREMISES)
 CONTROLLED BY APPLE)

Case: 2:20-mc-51089
 Judge: Parker, Linda V.
 Case No. Filed: 09-17-2020 At 12:02 PM
 IN RE:SEALED MATTER(SW)(MLW)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

See ATTACHMENT A.

located in the _____ Northern _____ District of _____ California _____, there is now concealed (*identify the person or describe the property to be seized*):

See ATTACHMENT B.

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

18 U.S.C. § 1347 & 1349

Health Care Fraud & Conspiracy to Commit Health Care Fraud

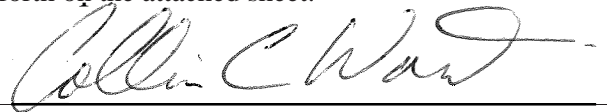
18 U.S.C. § 1343

Wire Fraud

The application is based on these facts:

See attached AFFIDAVIT.

- ☐ Continued on the attached sheet.
☐ Delayed notice _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

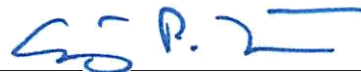
Collin Ward, Special Agent

Printed name and title

Sworn to before me and signed in my presence
 and/or by reliable electronic means.

Date: September 17, 2020

City and state: Detroit, Michigan



Judge's signature

Hon. Anthony P. Patti U. S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

IN THE MATTER OF
THE SEARCH OF

INFORMATION ASSOCIATED
WITH APPLE ID

tsyxxx@aol.com

THAT IS STORED AT PREMISES
CONTROLLED BY APPLE

Case No. _____

Case: 2:20-mc-51089

Judge: Parker, Linda V.

Filed: 09-17-2020 At 12:02 PM

IN RE:SEALED MATTER(SW)(MLW)

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Collin Ward, Special Agent for the Federal Bureau of Investigation, being duly sworn, depose and state as follows:

AGENT BACKGROUND AND QUALIFICATIONS

1. I make this Affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple Inc. (hereafter “Apple”) to disclose to the government records and other information, including the contents of communications, associated with the Apple ID tsyxxx@aol.com (“SUBJECT ACCOUNT”) that is stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at 1 Infinite Loop, Cupertino, CA. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B.

2. I am a Special Agent with the Federal Bureau of Investigation (“FBI”) and have been since May 2008. I currently am assigned to the Detroit FBI Office where I investigate

violations of federal law, specifically health care fraud and other financial crimes committed against federal government programs, such as the Medicare Program (“Medicare”). I am an investigative or law enforcement officer of the United States within the meaning of 18 U.S.C. § 2510(7), in that I am empowered by law to conduct investigations and to make arrests.

3. During my tenure with the FBI, I have participated in the execution of numerous search warrants related to health care fraud and other financial crimes, including fraud committed by medical practitioners against Medicare. Additionally, I have received training from the FBI and other sources in the investigation of health care fraud and other financial crimes. I have interviewed numerous medical doctors, medical providers, patients, and owners and employees of medical clinics. I have investigated and conducted surveillance on numerous doctors and medical providers. I have also received training and obtained experience in the use of computer technology and cellular telephones to further fraud investigations. As a result of my training and experience as a Special Agent with the FBI, my duties and responsibilities include criminal investigations into various federal statutes codified in the Federal Criminal Code and Rules. More specifically, my duties include investigating individuals and businesses who violated federal statutes and participate in billing both private insurance and government-sponsored health care programs, such as Medicare. These investigations have included individuals and businesses that have violated federal laws, including, but not limited to, Title 18, United States Code, Section 1347 (Health Care Fraud), Title 18, United States Code, Section 1349 (Conspiracy to Commit Health Care Fraud), Title 18, United States Code, Section 371 (Conspiracy to Pay and Receive Illegal Remunerations), and Title 42, United States Code, Section 1320a-7b(b) (Paying and Receiving Remunerations). In connection with investigating

these offenses, I have participated in the execution of search warrants for documents and other evidence in cases involving violations of these offenses.

4. I am conducting an investigation related to violations of the following statutes: 18 U.S.C. § 1347 (health care fraud); 18 U.S.C. § 1343 (wire fraud); 18 U.S.C. § 1349 (conspiracy to commit health care fraud and wire fraud); 18 U.S.C. § 371 (conspiracy to defraud the United States); 42 U.S.C. § 1320a-7b (Soliciting and Receiving Kickbacks Involving a Federal Health Care Program) (collectively, the “TARGET OFFENSES”).

5. As discussed herein, the statements in this Affidavit are based upon information I learned during the investigation, including information provided to me by other law enforcement agents, and my experience and background as an FBI Special Agent. Because this affidavit is being submitted for the limited purpose of supporting a search warrant, I have not included every fact known to me concerning this investigation. I have only set forth the facts I believe are necessary to establish probable cause to believe that evidence of crime, fruits of crime, contraband, and other items illegally possessed in violation of the aforementioned federal laws are contained in the SUBJECT ACCOUNT.

6. Based on the facts as set forth in this Affidavit, there is probable cause to believe that the SUBJECT ACCOUNT, described further in Attachment A, contains evidence, contraband, instrumentalities, and/or fruits of violations of the TARGET OFFENSES.

7. As discussed below, TRACEY SPENCER (“SPENCER”), RUBY SCOTT (“SCOTT”) and KYSHA MARSHALL (“MARSHALL”) and others known and unknown are believed to be engaged in a conspiracy to commit health care fraud and wire fraud, conspiracy to defraud the United States and to pay illegal kickbacks, related to the home health agency, Miracle Care LLC (“Miracle”), which is co-owned by SPENCER and SCOTT. The

investigation has thus far revealed that SPENCER and SCOTT, paid a patient recruiter and nurse, MARSHALL of Detroit Medical Center (“DMC”), illegal kickbacks in exchange for access to Medicare beneficiaries dating back to at least 2016. The investigation has also revealed that Miracle fraudulently billed Medicare for home health care services purportedly provided to Medicare beneficiaries who were not certified for home health care services by a physician. Between January 2013 and June 2020, Miracle billed Medicare approximately \$5,815,676.15 and was paid approximately \$6,867,247.83 by Medicare.

VIOLATION STATUTES

8. Title 18, United States Code, Section 1347 prohibits health care fraud: Whoever knowingly and willfully executes, or attempts to execute, a scheme or artifice –

- 1) to defraud any health care benefit program; or
- 2) to obtain, by means of false or fraudulent pretenses, representations, or promises, any of the money or property owned by, or under the custody or control of, any health care benefit program, in connection with the delivery of or payment for health care benefits, items, or services, shall be fined under this title or imprisoned not more than 10 years, or both.

9. Title 18, United States Code, Section 1343, prohibits wire fraud: “Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both.”

10. Title 18, United States Code, Section 1349 provides that any person who attempts or conspires to commit health care fraud and/or wire fraud shall be subject to the same penalties as those proscribed in 18 U.S.C. § 1347.

11. Title 18, United States Code, Section 24(b) defines a “health care benefit program” as, among other things, “any public or private plan . . . affecting commerce, under which any medical benefit, item, or service is provided to any individual, and includes any individual or entity who is providing a medical benefit, item, or service, for which payment may be made under the plan.”

12. Title 42, United States Code, Section 1320a-7b(b)(2)(A) prohibits knowingly and wilfully offering and paying any remuneration (including any kickback, bribe, or rebate) in return for referring an individual to a person for the furnishing or arranging of any item or service for which payment may be made in whole or part by Medicare, a federal health care benefits program as defined by 18 U.S.C. § 24(b).

13. Title 42, United States Code, Section 1320a-7b(b)(1)(A) prohibits knowingly and wilfully soliciting and receiving any remuneration (including any kickback, bribe, or rebate) directly or indirectly, overtly or covertly, in cash or in kind in return for referring an individual to a person for the furnishing or arranging for the furnishing of any item or service for which payment may be made in whole or part by Medicare, a federal health benefits program as defined by 18 U.S.C. § 24(b).

14. Title 18, United States Code, Section 371 provides that it a criminal offense “[i]f two or more persons conspire either to commit any offense against the United States, or to defraud the United States, or any agency thereof in any manner for any purpose.”

THE MEDICARE PROGRAM

15. The Medicare Program (“Medicare”) is a federally-funded health care program providing benefits to persons who are over the age of sixty-five or disabled. Medicare is administered by the Centers for Medicare & Medicaid Services (“CMS”), a federal agency within the United States Department of Health and Human Services (“HHS”). Individuals who receive Medicare benefits are referred to as Medicare “beneficiaries.”

16. Medicare is a “health care benefit program,” as defined by 18 U.S.C. § 24(b).

17. Medicare has four parts: hospital insurance (Part A), medical insurance (Part B), Medicare Advantage (Part C), and prescription drug benefits (Part D). Medicare Part B helps pay the cost of physician services, medical equipment and supplies, and other health services and supplies not paid by Part A.

18. This investigation involves home health care services. Home health care services typically include skilled nursing, physical therapy, and speech pathology services to homebound patients. Home health care services are covered by Medicare Part A.

19. Medicare claims for Part A are processed and paid by private insurance organizations known as fiscal intermediaries and carriers, respectively, who contract with CMS to administer their specific part of the Medicare program.

20. Medicare, through the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), requires a covered entity, such as a physician or home health care agency that bills Medicare, to retain required documentation for six years from the date of its creation or the date when it last was in effect, whichever is later.

21. Medicare will not pay for or reimburse services that are procured by kickbacks, in violation of Title 42, United States Code, Section 1320a-7b(b).

MEDICARE HOME HEALTH CARE REQUIREMENTS

22. Medicare's regulations for home health care services require a Home Health Agency ("HHA") be licensed by the state in which it is located, submit an application certifying it will follow the rules, regulations and laws applicable to Medicare, and be certified by a state agency. A qualified HHA receives a Medicare provider number that is used for the submission, processing, and payment of claims.

23. Medicare coverage for home health care services requires that the following qualifying conditions, among others, be met: (a) the Medicare beneficiary is confined to the home¹ and does not have a willing care-giver to assist him or her; (b) the beneficiary needs skilled nursing services, physical therapy, or occupational therapy; (c) the beneficiary is under the care of a qualified physician who established a written Plan of Care for the beneficiary, signed by the physician and by a Registered Nurse ("RN") (or therapist if only therapy services are provided) from the HHA; (d) skilled nursing services are provided by, or under the supervision of, an RN in accordance with the Plan of Care; and (e) the services provided are medically necessary.

24. To determine the proper level of care for a particular beneficiary, Medicare requires that HHAs perform a comprehensive initial evaluation, which includes a patient-specific, comprehensive assessment that accurately reflects the patient's current health and provides information to measure the patient's progress. Medicare requires that (a) an RN or qualified therapist perform the initial assessment (on an OASIS form), and (b) HHAs maintain a

¹ A beneficiary is homebound if he or she has a condition, due to an illness or injury, that restricts his or her ability to leave the home except with the aid of another individual or a supportive device, or if the beneficiary has a condition such that leaving his or her home is medically contraindicated.

clinical record of services they provide to each beneficiary, including signed and dated clinical and progress notes recording each home visit made to the beneficiary (“Visit Notes”). Visit Notes must include the identity of the individual who performed the visit, the name of the patient, and the type of service performed.

25. Medicare compensation to HHAs is based upon a prospective payment system (“PPS”). For every 60-day “episode” of services provided to each beneficiary, Medicare PPS pays HHAs a base payment that can be adjusted to reflect the severity of the beneficiary’s condition and care needs. Specifically, Medicare will pay 60% of the cost of the episode once the patient has been evaluated and a Plan of Care determined. At the end of the episode, Medicare pays the balance based on how much therapy was actually provided in the episode. If the beneficiary is still eligible for care at the end of an episode, a second episode of services can be provided. Each subsequent episode must be based upon a new OASIS, wherein the beneficiary’s physician and RN (or therapist) re-certifies the beneficiary’s medical condition, need for services, and a new Plan of Treatment. The OASIS re-certification must be approved by the patient’s physician and an RN (or therapist) from the HHA.

SUBJECT ACCOUNT

26. Records relating to the SUBJECT ACCOUNT were obtained from Apple via subpoena. The records list SPENCER as the account holder for the SUBJECT ACCOUNT and list her address as 22067 Saskatoon Ct., Macomb, MI. The SUBJECT ACCOUNT was created on March 4, 2011. The daytime phone number on the account is listed as (586) 549-4642 (“SPENCER CELL PHONE 1”) and the “Facetime/iMessage Phone” is listed as SPENCER CELL PHONE 1 and (586) 460-5900 (“SPENCER CELL PHONE 2”).

FACTS SUPPORTING PROBABLE CAUSE

Miracle Care LLC d/b/a Phenomenal Home Health Care

27. According to Miracle's provider enrollment, chain and ownership ("PECOS") data, Miracle is a Medicare enrolled home health agency with a mailing address and primary practice location of 2727 2nd Avenue, Suite 121, Detroit, Michigan 48201. The PECOS records reflect that SPENCER has been associated with Miracle since April 12, 2011, and has listed roles of Director, W-2 Managing Employee, Authorized Official, 5% or Greater Direct Ownership Interest, and Officer.² The exact ownership percentage is listed at 50%. SPENCER, along with SCOTT, who is also listed as having a 50% ownership interest, are listed as the Authorized Officials. SPENCER is also listed as the Contact Person. Under the section "Certification Records," SPENCER's name is listed several times with telephone numbers associated with her as SPENCER CELL PHONE 1 and (313) 974-6480.³

Macomb County Sherriff's Office Homicide Investigation

28. In the early morning hours of May 6, 2017, the Macomb County Sherriff's Office was called to SPENCER's home address in response to a report of a shooting. Based on the initial investigation by the Macomb County Sherriff's Office, it was determined that SPENCER had shot and killed her boyfriend in a domestic dispute.

² According to corporate records obtained from the Michigan Department of Licensing and Regulatory Affairs ("LARA") via subpoena, SPENCER is also listed as the CEO, registered agent and a member of Miracle.

³ According to subscriber records obtained from Comcast via subpoena, telephone number (313) 974-6480 is subscribed to by Phenomen [sic] Home Health, with a service address of 2727 2nd Avenue, Ste 121, Detroit, Michigan 48201. According to Miracle's PECOS data, Phenomenal Home Health Care ("Phenomenal") is a Doing Business as Name for Miracle Care LLC.

29. On May 15, 2017, Detective John Becker of the Macomb County Sheriff's Office provided the following information to a Special Agent with the FBI:

- a. During the course of an initial homicide investigation, investigators executed a search warrant at SPENCER's residence and found approximately \$270,000 in cash. There was approximately \$29,000 in cash found in one of the bedrooms and approximately \$240,000 in cash located within a safe in SPENCER's closet. When Detective Becker inquired about the large amount of cash, SPENCER advised she did not know anything about the \$29,000, believing it belonged to her boyfriend, and indicated the \$240,000 in her bedroom closet safe was used to pay her employees.
- b. Detective Becker indicated that investigators found Medicare and Medicaid forms haphazardly filled out and strewn throughout SPENCER's home office.
- c. Records from the Macomb County Sheriff's Office indicated that two Apple iPhones were also seized from SPENCER's residence during the execution of the search warrant.⁴ During the course of the investigation, SPENCER told officers that she owns a home care company. SPENCER's sister, A.J. of Jonesboro, Georgia, was also interviewed in connection with the investigation.

30. Later in his investigation, Detective Becker obtained a search warrant for one of the Apple iPhones seized from SPENCER's residence by the Macomb County Sheriff's Office. While reviewing SPENCER's text messages,⁵ Detective Becker came across a large number of

⁴ The Apple iPhones are still in the custody of the Macomb County Sheriff's Office.

⁵ Affiant contacted the Macomb County Sheriff's Office to inquire if a cellular telephone analysis was completed and was available within their file. The detective currently assigned to the SPENCER case (Detective Becker has since retired) was unable to locate a completed

communications between SPENCER and what appeared to be SPENCER's employees and/or marketers, based on the content of the text communications.⁶ The messages covered a range of topics to include the number of patient visits employees made on certain dates and their concern that if they submitted too many hours it may look suspicious. Other text messages discussed the number of referrals provided. Detective Becker advised that one of the communications was between SPENCER and telephone number (248) 242-0164, a number Detective Becker indicated belonged to MARSHALL who was an employee at DMC. In the course of the communication, MARSHALL discussed the hundreds of referrals she sent to SPENCER's business and that she just needs some of the patients to sign up so she can get paid. A number of patient names were also passed via text message between SPENCER and possible employees, discussing what patients were seen by what employees on certain dates.

31. To date, SPENCER has not been charged with any crimes in connection with the shooting.

Miracle Investigation

32. A query of an open source commercial database confirmed that telephone number (248) 242-0164 ("MARSHALL CELL PHONE") was associated with MARSHALL. On August 24, 2020, affiant did a Google search of "Kysha Marshall" and the first search result was a LinkedIn page for a Kysha Marshall. A review of the LinkedIn page listed Kysha Marshall as being an RN Case Manager at DMC from April 2008 to the present.

forensic analysis of SPENCER's cellular telephone within their file.

⁶ Based on my training and experience investigating health care fraud case, I know that a "marketer" is a common phrase for someone who refers patients to home health agencies.

33. Investigators obtained bank records for Miracle and SPENCER via subpoena. A review of a Bank of America account in the name of Miracle and SPENCER, account ending in 0470, identified transactions where money was being sent to MARSHALL. A review of the details section of the transactions indicated that the money transfer transaction was completed utilizing a money transfer application, believed to be the Square Cash App (“Cash App”).

34. According to an internet article appearing on the Business Insider internet page on January 2, 2020, titled, “How does Cash App work?: Cash App’s primary features, explained,” the Cash App is an app for sending and receiving money.⁷ The article explains users of the Cash App can create a free account that will then let them instantly send or receive money from other users within the same country. Once the user downloads the Cash App, the user chooses a unique username. Users can also be found using the phone number or email address tied to their account. The article further states that the Cash App has two primary functions: paying people and getting paid.

35. According to the “About this app” section under the Cash App in Google Play Store, the Cash App was initially released on October 15, 2013, and the application is offered by Square, Inc.

36. Finally, I know based on my training and experience that the Cash App, formerly known as Square Cash, is a mobile payment service allowing users to transfer money to one another using a mobile phone app.

37. Investigators obtained records in February 2020 and June 2020 from Square Inc. for SPENCER and MARSHALL via subpoena. The subscriber info on SPENCER’s accounts includes her phone number as SPENCER CELL PHONE 1 and SPENCER CELL PHONE 2 and

⁷<https://www.businessinsider.com/how-does-cash-app-work> (last viewed on August 20, 2020).

lists her email address as sabarriel@gmail.com. The subscriber info on MARSHALL's account includes her phone number as MARSHALL CELL PHONE.

38. Records from Google list "T Spencer" as the subscriber for the email address sabarriel@gmail.com. SPENCER CELL PHONE 1 is listed as the account recovery SMS phone number and tsyxxx@aol.com is listed as the alternate email address on the account.

39. A review of the Cash App records for MARSHALL indicated that both SPENCER and SCOTT utilized the Cash App to send money to MARSHALL. From May 25, 2016 to June 24, 2018, SPENCER paid MARSHALL 121 times via the Cash App totaling approximately \$33,980.00, including approximately 108 of the 121 total payments being in an amount that was a multiple of \$200. From July 6, 2018 to June 25, 2020, SCOTT paid MARSHALL 51 times via the Cash App totaling \$47,170.00. In all, SPENCER and SCOTT sent MARSHALL \$81,150.00 in 172 separate transaction between May 25, 2016 and June 25, 2020 via the Cash App. Many of the transactions, however not all of them, contained a subject. A sample of some of the transactions and their subjects from the Cash App information are below:

Date	Amount	Subject	Sender	Recipient
2019-06-21 13:46:17 UTC	1,200.00	referrals	Ruby Scott	Kysha Marshall
2018-07-26 12:39:00 UTC	300.00	rent	Ruby Scott	Kysha Marshall
2017-10-13 18:21:31 UTC	465.00	2 SOC AND ONE REVISIT	Tracey Spencer	Kysha Marshall
2017-05-12 23:28:49 UTC	460.00	2 opens and one revisit LC HOPES AMD REGINA M	Tracey Spencer	Kysha Marshall
2017-04-21 20:39:35 UTC	400.00	[J.T.] is open, [W.T.] is open	Tracey Spencer	Kysha Marshall

2017-01-05 02:39:49 UTC	200.00	[T.L.]	Tracey Spencer	Kysha Marshall
2016-11-15 15:59:30 UTC	200.00	Townsville	Tracey Spencer	Kysha Marshall
2016-11-07 23:31:01 UTC	200.00	hardyway	Tracey Spencer	Kysha Marshall
2016-05-25 16:52:58 UTC	200.00	work	Tracey Spencer	Kysha Marshall

40. As seen in the table above, the Cash App transactions contain a variety of descriptions within the subject field to include referrals, rent, SOC (based on my training and experience believed to reference start of care), revisits, opens, work, and what appear to be patient names. In fact, a review of Miracle's Medicare Part A billing data for the names listed in the above table, showed that those names were Medicare beneficiaries who purportedly received home health services from Miracle. While it is possible that MARSHALL, as a nurse, could be receiving payment for nursing services provided as part of a legitimate home health care visit, based on my training and experience investigating home health care fraud, it would seem unlikely the payment for such legitimate services would be made via the Cash App instead of via a W-2 payroll check or 1099 contractor payment. Also, the individual \$200 payments being made in late 2016 and early 2017 as part of a transaction that has a patient name as the subject, is, based on my training and experience, indicative of an illegal kickback payment. The \$200 payment is indicative of a kickback payment due to the round dollar number of the payment, indicating a possible per patient payment rate, as well as the fact those round dollar number payments had subject descriptions that included patient names. Further, the first payment in the table above specifically lists "referrals" in the subject line of the transaction. Based on my training and experience investigating home health care fraud, owners of home health care agencies who make payments to individuals, especially in even dollar increments, where the payments reference referrals are indicative of illegal kickback payments.

41. As indicated above, MARSHALL's LinkedIn page indicated that she was an RN Case Manager at DMC. A Medicare data shared beneficiary report was run for Medicare beneficiaries who had Medicare billings at both DMC – Detroit Receiving Hospital and Miracle. This report indicated there were approximately 286 Medicare beneficiaries who had Medicare billings at both DMC – Detroit Receiving Hospital and Miracle. Of those 286 Medicare beneficiaries, approximately 56 were identified in the subject line of Cash App payments from SPENCER to MARSHALL. Based on my training and experience investigating home health care fraud, this data is relevant because it corroborates that MARSHALL was paid by SPENCER via the Cash app for referring patients from DMC – Detroit Receiving Hospital to Miracle. In total, Miracle billed Medicare approximately \$170,191.24 and was paid \$240,618.00 by Medicare from about June 10, 2016 to June 30, 2018 in connection with claims for purported home health services for those 56 patients identified in the subject line of Cash App payments from SPENCER to MARSHALL. In analyzing the Cash App subject line to identify Medicare beneficiaries there were instances where the subject line contained a first name and last name. However, there were also instances where only a last name or what affiant believed to be a misspelled name appeared on the Cash App subject line. In those instances, affiant used the last name or likely misspelled name from the Cash App subject line and compared it to the names in the Medicare data of the shared beneficiary report. In order to determine if the last name or likely misspelled name from the Cash App subject line related to a specific Medicare beneficiary from the shared beneficiary report, affiant compared the payment date from the Cash App to the start date for the home health care episode from the shared beneficiary report. If affiant was able to match a last name or likely misspelled name from the Cash App to the start date from the shared beneficiary report within several days or a week or two of each other than those Medicare

beneficiaries were included in the 56 identified Medicare beneficiaries referenced above.

Examples of a few of these are as follows with the below data being from the Cash App data and

Medicare data:

	Date	Amount	Subject	Sender	Recipient
Cash App	2018-05-11 19:44:35 UTC	200.00	[D.] Carvin	Tracey Spencer	Kysha Marshall

	Episode Start	Episode End	Medicare Beneficiary	Billed by Miracle	Paid to Miracle
Medicare	5/1/2018	5/15/2018	[D.] Carvin	\$1,030.01	\$1,606.86

	Date	Amount	Subject	Sender	Recipient
Cash App	2016-10-28 19:37:55 UTC	200.00	WILLIAMS	Tracey Spencer	Kysha Marshall

	Episode Start	Episode End	Medicare Beneficiary	Billed by Miracle	Paid to Miracle
Medicare	10/27/2016	12/25/16	[A.] Williams	\$2,320.01	\$2,881.34
	Date	Amount	Subject	Sender	Recipient
Cash App	2016-06-30 15:41:27 UTC	200.00	Mckinsery	Tracey Spencer	Kysha Marshall

	Episode Start	Episode End	Medicare Beneficiary	Billed by Miracle	Paid to Miracle
Medicare	6/29/2016	8/13/16	[A.V.] McKinsty	\$1,220.01	\$1,987.84

	Date	Amount	Subject	Sender	Recipient
Cash App	2016-06-12 13:38:14 UTC	200.00	hodg	Tracey Spencer	Kysha Marshall

	Episode Start	Episode End	Medicare Beneficiary	Billed by Miracle	Paid to Miracle
Medicare	6/10/2016	6/24/16	[J.] Hodges	\$140.01	\$222.13

42. In summary, given the Cash App information shows payments being made from Miracle owners, SPENCER and SCOTT,⁸ to MARSHALL and many of these payments contain subject descriptions that specifically name Medicare beneficiaries that purportedly received services from Miracle and by which Miracle billed and/or received reimbursement from Medicare for those services, this is evidence of illegal kickback payments.

Text Communications between SPENCER and MARSHALL

43. As previously stated, according to the PECOS data, SPENCER is listed as the contact person for Miracle and one of her phone numbers is listed as SPENCER CELL PHONE 1. According to records from AT&T Wireless (“AT&T”) SPENCER is listed as the subscriber for SPENCER CELL PHONE 1, since September 12, 2007 through the date of the most recent records from AT&T, May 25, 2020.

44. As previously stated, on May 6, 2017, an Apple iPhone was seized from SPENCER’s residence by the Macomb County Sherriff’s Office in connection with the homicide investigation.

45. As previously stated, one of the text messages that Detective Becker of the Macomb County Sherriff’s Office saw on the device was between SPENCER and the MARSHALL CELL PHONE, a number Detective Becker indicated belonged to MARSHALL. Records were obtained from T-Mobile relating to the MARSHALL CELL PHONE via subpoena. The records list J.M. of 33359 Elgin Court, Sterling Heights, Michigan as the subscriber on the account.⁹ Subscriber records from Square for the Cash App relating to

⁸ Since about May 2018, Ruby Scott is also listed in Medicare documents as an owner of Delta Home Health Care LLC, another home health agency that is also a Medicare enrolled provider and located in Canton, Michigan.

⁹ According to an open source commercial database search of J.M. and MARSHALL, they were

MARSHALL list her phone number as MARSHALL CELL PHONE and one of the addresses listed on her account is also 33359 Elgin Court, Sterling Heights, Michigan.

46. The AT&T records relating to SPENCER CELL PHONE 1 revealed that from April 20, 2016 to May 6, 2017, there were approximately 1,375 text messages exchanged between SPENCER CELL PHONE 1 and MARSHALL CELL PHONE, including approximately 584 text messages between the two phones on days where SPENCER paid MARSHALL via the Cash app.

47. Records relating to SPENCER CELL PHONE 2 were obtained from AT&T via subpoena. The records reflect that the account was created on May 9, 2017, and the subscriber is listed as SPENCER'S sister, A.J. of Jonesboro, Georgia. Jones' home phone number is listed as (111) 111-0001 and work phone number is listed as (111) 111-0002. However, the email address listed on the account is sabarrie1@gmail.com, which has been previously identified as SPENCER'S email address. The first payment on the account for SPENCER CELL PHONE 2 on was made on May 9, 2017 on a credit card in SPENCER'S name.

48. According to records from Apple for SUBJECT ACCOUNT, on May 9, 2017, two Apple iPhones were purchased and one of the Apple iPhones was also registered to the SUBJECT ACCOUNT on May 9, 2017.

49. I know based on my training and experience, that a phone number can be transferred from one device to another.

both associated with two residence addresses during a reported time period that overlapped. Based on that, and other open source materials and records relating to MARSHALL'S 2015 bankruptcy proceeding in the Eastern District of Michigan, it is believed that J.M. is MARSHALL'S daughter.

50. According to AT&T phone records for SPENCER CELL PHONE 1, there is only one outgoing text message or phone call between May 6, 2017, 6:27 GMT until May 9, 2017, 16:22 GMT which occurred on May 8, 2017, 19:17 GMT. Also, according to AT&T phone records for SPENCER CELL PHONE 1, there was no data usage for SPENCER CELL PHONE 1 on May 7, 2017 and May 8, 2017.

51. Based on all of this, it appears to this affiant that most likely on May 9, 2017, SPENCER purchased two new Apple iPhones and registered at least one of them to the SUBJECT ACCOUNT. Based on my training and experience, it appears that one of those Apple iPhones was then assigned SPENCER CELL PHONE 1 (from the phone that was in custody of the Macomb County Sherriff's Office) and the other was assigned SPENCER CELL PHONE 2.

52. Based on records from AT&T, SPENCER CELL PHONE 2 and MARSHALL CELL PHONE exchanged approximately 3,732 text messages between May 9, 2017 and March 2, 2020. Between May 12, 2017 and June 24, 2018, SPENCER paid MARSHALL via the Cash App approximately 56 times taking place across 51 different dates. SPENCER CELL PHONE 2 and MARSHALL CELL PHONE exchanged text messages on all 51 days that SPENCER paid MARSHALL during this period, totaling approximately 452 text messages exchanged across the 51 days.

Cooperating Witness

53. On August 13, 2019, Dr. Solomon Awusah¹⁰ ("Awusah") was interviewed and he provided the following information related to SPENCER and Miracle:

¹⁰ On June 21, 2018, Awusah was indicted on two counts of conspiracy to defraud and pay and receive kickbacks, in violation of 18 U.S.C. § 371 and two counts of receipt of kickbacks in violation of 42 U.S.C. §1320a-7b(b)(1)(a). He was arrested on June 26, 2018. On July 25, 2019, Awusah pled guilty to one count of conspiracy to pay and receive kickbacks, in violation of 18 U.S.C. § 371 and entered into a cooperation agreement. Awusah has not yet been sentenced.

- a. Awusah was not familiar with a home health care company called Miracle, however, he was familiar with SPENCER and knew her as the owner of Phenomenal Home Health Care.¹¹ Awusah never heard of Miracle as it related to SPENCER, he only knew of Phenomenal. Phenomenal would send 485s (also known as a Home Health Certification and Plan of Care)¹² to Awusah's physician practice, Maecenas Health Systems, for patients Awusah did not know. Phenomenal would indicate those 485s were sent to Awusah by mistake.
- b. In 2015, Awusah was trying to start a romantic relationship with SPENCER and they also talked about business. SPENCER told Awusah she was going to send him a lot of patients, but according to Awusah, she never did. Awusah only referred SPENCER a handful of patients. Awusah remembered at least two specific patients that were referred to SPENCER and those patients may have been re-certified for home health care. Awusah could not remember the names of the two patients but believed they lived on the west side of Detroit, Michigan. There was no monetary agreement between Awusah and SPENCER for the referral of patients. Awusah believed his last referral to SPENCER was in 2018 prior to his indictment and arrest.

¹¹ Per Footnote 3 above, Phenomenal Home Health Care is a doing business as name for Miracle.

¹² Based on my training and experience investigating home health care fraud, I know that a Form 485 is a CMS form that documents medical information about a Medicare beneficiary and documents a physician's order for home health care treatment as well as the physician's certification that the Medicare beneficiary is homebound and needs the home health care services being ordered.

- c. Awusah believed it was possible that his office manager might have put home health care referral documentation in front of him to sign. However, Awusah said any legitimate home health care patient referral sent by him would have corresponding Medicare Part B claims from him for a physician visit with that patient. Awusah indicated that if Medicare claims data indicated that a patient was referred for home health care by him and there were no corresponding Medicare Part B claims billed by him, then he did not send that referral.
54. On August 21, 2020, Awusah confirmed he never sent any home health care referrals after the date of his arrest. As mentioned in a previous footnote, the date of Awusah's arrest was June 26, 2018.
55. On December 9, 2019, Awusah was interviewed and provided the following information about SPENCER:
- a. Awusah believed he only saw and referred two or three patients for SPENCER's company. At most, Awusah may have referred ten patients and maybe there were two or three re-certifications for home health care. Awusah recalled his office receiving random 485s from SPENCER's company for patients Awusah had never heard of. Awusah told his office staff to follow up about these patients, which Awusah assumed they did. Awusah wanted business from SPENCER, but the business never came through.
56. Medicare claims data indicates that Awusah was the top referring provider of beneficiaries to Miracle for home health services from December 11, 2014 to April 9, 2019, referring approximately 166 individual Medicare beneficiaries for approximately 274 episodes of

home health care services. These referrals resulted in Miracle billing Medicare approximately \$470,302.73 and Medicare paying Miracle approximately \$601,417.76.

57. Medicare claims data indicates that Awusah was listed as the referring provider on claims for home health services purportedly rendered by Miracle for approximately 106 individual Medicare beneficiaries for approximately 130 episodes of home health where Awusah did not bill Medicare Part B for his physician services. Miracle billed Medicare approximately \$148,051.23 and Medicare paid Miracle approximately \$220,200.82 in connection with these claims.

58. Furthermore, Medicare claims data indicates that Awusah was purportedly the referring provider on claims for home health services submitted by Miracle for four Medicare beneficiaries **after** Awusah was indicted and arrested in June 2018. The following table summarizes the claims:

Beneficiary Initials	Start Date	End Date	Billed by Miracle	Paid to Miracle
R.H.	7/25/18	9/22/18	\$6,055.01	\$3,928.22
M.F.	8/2/18	8/2/18	\$250.01	\$243.3
M.N.	12/13/18	2/10/19	\$2,000.01	\$1,621.43
K.G.	2/23/19	4/9/19	\$2,730.01	\$1,239.67
Total			\$11,035.04	\$7,032.62

59. Furthermore, an analysis was performed between Awusah's Medicare claims data and the information from the Cash App records. Based on this analysis, investigators identified at least 19 Medicare beneficiaries that: (1) were identified in the Cash App subject line on payments made from SPENCER to MARSHALL, (2) were referred to Miracle for home health care by Awusah, (3) had claims for purported home health services billed to Medicare by Miracle and (4) did not have any Medicare Part B billings by Awusah. For the 19 Medicare

beneficiaries that met the above criteria, Miracle billed Medicare \$27,940.19 and Medicare paid Miracle \$41,115.48 from approximately June 10, 2016 to March 19, 2018.

Text Communications between Cooperating Witness and SPENCER

60. As part of a separate investigation, Federal Agents obtained a search warrant for Awusah's cellular telephone. Awusah's cellular telephone was forensically examined for data and communications, such as text messages. Awusah's cellular telephone contained text messages with SPENCER, the first of which was on October 23, 2014, and the last text communication was before the shooting on May 6, 2017. During these text communications, SPENCER utilized the telephone number affiliated with SPENCER CELL PHONE 1. The text message communications demonstrate that Awusah and SPENCER discussed patient referrals via text. Examples of text communications between Awusah and SPENCER that are relevant to this investigation are as follows:

- a. On or about December 4, 2014, Awusah texted SPENCER, "You can have your co-ordinator [sic] call and ask for Flora. Tell them that it has been ok'ed by Dr. Solomon." Based on the separate investigation, affiant knows Flora to be the first name of a previous office manager who worked at Awusah's physician practice. Also, based on my knowledge and experience investigating home health care fraud, the reference to "your co-ordinator" is likely a reference to an employee who works at SPENCER's home health care company and, thus, Awusah is likely telling SPENCER to have her employee contact his office manager.

61. On or about December 11, 2014, SPENCER texted Awusah, "[five emojis] baby do u go to Pontiac" followed by "And thank u for referral." Awusah responded to SPENCER, "Awwwwww sweetie, u know, u r my girl" and "We go to Pontiac if we have multiple patients to see

there on that day for logistics reasons.” SPENCER then responded to Awusah, “Oh yes I understand kisses [four emojis].” Based on my training and experience investigating home health care fraud, this text message conversation appears to be SPENCER asking Awusah if he sees patients in Pontiac while also thanking Awusah for a referral. Awusah responds to SPENCER, in part, by saying “We go to Pontiac if we have multiple patients to see...,” which seems to be a clear reference by Awusah to his physician practice. The text conversation also contains language and emojis that would more likely be included in personal, rather than business, conversations, however, as Awusah stated to investigators he was trying to have a personal, romantic relationship with SPENCER as well as a business relationship.

62. On or about December 18, 2014, SPENCER texted Awusah, “Hey baby the patient [L.N.] requested for us to open her the day after XMAS.” A review of Awusah’s Medicare Part B billing data shows that L.N. was seen by Awusah on or about December 1, 2014. However, a review of Miracle’s Medicare Part A billing data does not show a home health care episode for L.N. at Miracle. Despite Medicare Part A billing data not showing any services provided to L.N. by Miracle, the text message does show SPENCER utilized SPENCER CELL PHONE 1 to communicate with Awusah about a patient.

63. On or about August 13, 2015, Awusah texted SPENCER, “[B.H.] is dead, and I will fax the rest of the f2f for [R.G.] and [M.I.].” Based on my training and experience investigating home health care fraud, “f2f” likely refers to a face to face encounter form that is a document for home health care. A review of Awusah’s Medicare Part B billing data showed billing for both R.G. and M.I. Also, a review of Miracle’s Medicare Part A billing data showed billings for both R.G. and M.I. Specifically, Miracle’s Medicare Part A billing data showed, in part, home health care episodes from June 25, 2015 to August 23, 2015 and August 24, 2015 to

September 30, 2015 for R.G. as well as home health care episodes from May 27, 2015 to July 14, 2015 and August 7, 2015 to September 29, 2015 for M.I. Miracle's Medicare Part A billing data also listed Awusah as the referring physician for the aforementioned home health care episodes of R.G. and M.I.

INFORMATION REGARDING APPLE ID AND iCloud¹³

64. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

65. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

- a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.
- b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

¹³ The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at <http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf>; "Manage and Use Your Apple ID," available at <https://support.apple.com/en-us/HT203993>; "iCloud," available at <http://www.apple.com/icloud/>; "What does iCloud back up?," available at <https://support.apple.com/kb/PH12519>; "Apple Platform Security," available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and "What is iCloud?," available at <https://support.apple.com/kb/PH26502>.

- c. iCloud is a file hosting, storage, and sharing service provided by Apple.

iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

- d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-

connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com.

iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers.

iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to

synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iWork Apps, a suite of productivity apps

(Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain

enables a user to keep website username and passwords, credit card

information, and Wi-Fi network information synchronized across multiple

Apple devices. The iCloud Backup feature enables a user to have a copy of the information on their Apple devices saved in the iCloud including

iMessage, text (SMS), and MMS messages.

- e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.
- f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.
- g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.
- h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

66. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

67. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to

access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a “verification email” sent by Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an Apple ID by the user.

68. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user’s full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the “My Apple ID” and “iForgot” pages on Apple’s website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address (“IP address”) used to register and access the account, and other log files that reflect usage of the account.

69. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user’s sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple’s website. Apple also maintains records reflecting a user’s app purchases from App Store and iTunes Store, “call invitation logs” for FaceTime calls, “query logs” for iMessage, and “mail logs” for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

70. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

71. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated

with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

72. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. Specifically, the evidence above shows that SPENCER, used an app, the Cash App, on her iPhone to pay MARSHALL what are believed to be illegal kickbacks. Additionally, that SPENCER and MARSHALL were in regular communication via text messages over the course of the years where SPENCER and SCOTT were paying MARSHALL what are believed to be illegal kickbacks, including on the majority of the dates where the payments were made. Additionally, I know that SPENCER was in contact via text message with Awusah about Medicare patient referrals to Miracle.

73. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. As noted above, SPENCER and MARSHALL regularly used iMessage/text messages to communicate, including on the dates where SPENCER paid

MARSHALL via the Cash app. Likewise, SPENCER spoke to Dr. Awusah about patient referrals to Miracle.

74. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the SUBJECT ACCOUNT. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

75. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

76. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages,

Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

77. As previously stated, records relating to the SUBJECT ACCOUNT were obtained from Apple via subpoena. The records list SPENCER as the account holder for the SUBJECT ACCOUNT and list her address as 22067 Saskatoon Ct., Macomb, MI. The SUBJECT ACCOUNT was created on March 4, 2011. The Account Type is listed as “Full iCloud.” The daytime phone number on the account is listed as (586) 549-4642, SPENCER CELL PHONE 1, and the “Facetime/iMessage Phone” is listed as SPENCER CELL PHONE 1, and SPENCER CELL PHONE 2. The SUBJECT ACCOUNT has the following iCloud features:

- Bookmarks
- Calendars
- Contacts
- Find my Friends
- iCloud Backup (ios Devices)
- iCloud Drive
- iCloud Photos
- Mail
- Notes

78. As previously stated, the iCloud Backup feature enables a user to have a copy of the information on their Apple devices saved in the iCloud including iMessage, text (SMS), and MMS messages.

79. According to records from Apple, the last time that the SUBJECT ACCOUNT was backed up to the iCloud was August 14, 2020.

80. Therefore, Apple’s servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple’s services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account’s user or users.

81. Based on my training and experience, along with the information described above, there is probable cause to believe that the iPhones connected to the SUBJECT ACCOUNT were used in order to further the crimes described above, the TARGET OFFENSES, and that evidence of those crimes, including data, text messages, and information related to the Cash app, are contained in the SUBJECT ACCOUNT. In addition, in my experience, conspirators in illegal fraud schemes utilize cellular telephones to communicate about the scheme.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

82. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

SPECIAL INSTRUCTIONS REGARDING REVIEW OF SEIZED MATERIALS

83. With respect to law enforcement's review of the seized material identified in Attachment B, law enforcement (i.e., the federal agents and prosecutors working on this investigation and prosecution), along with other government officials and contractors whom law enforcement deems necessary to assist in the review of the seized material (collectively, the "Review Team") are hereby authorized to review, in the first instance, the seized material.

84. If, during the review of the seized material, the review team finds potentially privileged materials, the review team will: (1) immediately cease its review of the potentially

privileged materials at issue; (2) segregate the potentially privileged materials at issue; and (3) take appropriate steps to safeguard the potentially privileged materials at issue. Nothing in this Instruction shall be construed to require the Review Team to cease or suspend review of all the seized material upon discovery of the existence of potentially privileged materials within a portion of the seized material.

CONCLUSION

85. Based on the forgoing, I request that the Court issue the proposed search warrant.

86. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offenses being investigated.” 18 U.S.C. § 2711(3)(A)(i).

87. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

REQUEST FOR SEALING

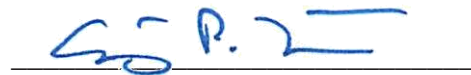
88. I respectfully request that the Court order that all papers in support of this application, including the affidavit and search warrants, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize the investigation and its effectiveness.

A handwritten signature in black ink, reading "Collin C. Ward", is positioned above a horizontal line.

Special Agent Collin C. Ward

Federal Bureau of Investigation

Sworn to before me and signed in my
presence and/or by reliable electronic means.

A handwritten signature in blue ink, reading "Hon. Anthony P. Patti", is positioned above a horizontal line.

Hon. Anthony P. Patti

United States Magistrate Judge

Eastern District of Michigan

Dated: September 17, 2020

ATTACHMENT A – PROPERTY TO BE SEARCHED

This warrant applies to information associated with the Apple ID tsyxxx@aol.com (the “SUBJECT ACCOUNT”) that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014, from October 23, 2014 to present.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for the account listed in Attachment A, from October 23, 2014, to the present:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP

addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

d. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

e. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

f. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

g. All records pertaining to the types of service used;

h. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

i. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

The Provider is hereby ordered to disclose the above information to the government within no later than **fourteen (14) days** of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes contraband, fruits, evidence and/or instrumentalities of violations of 18 U.S.C. §§ 1347, 1343, 1349, and 371 and 42 U.S.C. §§ 1320a-7b(b)(2)(A) and 1320a-7b(b)(1)(A) (“the Target Offenses”) involving Tracey Spencer, Apple ID account tsyxxx@aol.com, from October 23, 2014 to the present, including information pertaining to the following matters:

- a. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);
- b. Any and all location information about the geographic location of the user of the Apple ID;
- c. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the Target Offenses and the account subscriber;
- d. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);
- e. Records relating to the of download and use of apps from the App store;
- f. Evidence indicating the subscriber’s state of mind as it relates to the Target Offenses; and
- g. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

**CERTIFICATE OF AUTHENTICITY OF
DOMESTIC BUSINESS RECORDS PURSUANT TO
FEDERAL RULE OF EVIDENCE 902(11)**

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Apple Inc., and my official title is _____ . I am a custodian of records for Apple Inc. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Apple Inc., and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;
- b. such records were kept in the ordinary course of a regularly conducted business activity of Apple Inc.; and
- c. such records were made by Apple Inc. as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date

Signature

Hon. Anthony P. Patti U. S. Magistrate Judge
Printed name and title

Return

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

*Executing officer's signature*_____
Printed name and title